



## A NOVEL APPROACH OF COMBINING STEGANOGRAPHY ALGORITHMS

Hamdan Lateef Jaheel and Zou Beiji

School of Information Science and Engineering, Central South University,  
Hunan, P.R. China

---

*Submitted: Nov. 3, 2014*

*Accepted: Jan. 5, 2015*

*Published: Mar. 1, 2015*

---

*Abstract- Steganography is the act of hiding a message inside another message in such a way that the hidden message can only be detected by its intended recipient. In this paper, we combined two steganography algorithms namely JSteg and OutGuess algorithms, in order to exploit the beneficial characteristics and features of both algorithms to enhance the protection level for secret images. In our proposed approach, the secret message (image) is first concealed inside another image using JSteg algorithm and the resultant stego-image is further hidden inside a final image using OutGuess 0.1 algorithm. In this combine approach, the tricky nature of hiding an already hidden message is using two different algorithms increases the level of difficulty for a third party to suspect the existence of a secret image in the first place or even successful decode the it. Besides that, the priority given to the choice of a good image size and type in this approach further disguises the secret image and increases the chances that the image could go unnoticed. Results after calculating the capacity and PSNR for images proved that our approach is a good and acceptable steganography system. The model presented here is based on JPEG images.*

**Index terms:** Transform Domain Technique, Jsteg, OutGuess0.1, MSE , peak-signal-to-noise ratio (PSNR).

## I. INTRODUCTION

Steganography refers to the art and science of hiding communication. It is through the application of information hiding that made it possible for Alice send a secret message (image, audio, text) to Bob in a manner that any third party will not know the message exist in the first place. Usually, hiding a message (image, audio, text) inside another median (image, audio, text or video) known as a covered work and modifying its properties during the process produces what is called a stegogramme. The stegogramme contains the secret message in an unnoticeable manner. It is this stegogramme that is sent from Alice to Bob. If anyone intercepts the communication, they will obtain the stegogramme, but as it is so similar to the cover, it is a difficult task for them to say that the stegogramme is anything but innocent. It is therefore the duty of steganography to ensure that the adversary regards the stegogramme, and thus the communication as innocuous. Steganography is not a new topic which is considered these days, its history can be traced in 440 BC. Herodotus, a Greek historian from the 5th Century BC, In the first usage of this knowledge the secret messages were written on the shaved head of Greek soldiers, when their hair grew up, the messages were concealed from the others. These days, computer and network technologies provide easy to use communication channels for steganography, where images, audio and video files can be used as a cover media[1].

On one hand, steganography is usually applied computationally, when cover works such as digital media (text files, image files, audio files, and video files) are tweaked in such a way that a secret message can be concealed inside them.

The techniques are very similar to that of digital watermarking, but there is a big difference between the two. In watermarking system's the main objective is to achieve a high level of robustness such that it should be impossible to remove a watermark without degrading the quality of the data object. Steganography rather focuses on making it extremely difficult to tell whether a secret message exists at all or not. If an unauthorised third party is able to say with high confidence that a file contains a secret message, then steganography has failed [2].

There are many reasons why steganography is used. Mainly it insures the possibility of sending secret messages even under monitored conditions. There are many different ways of sending messages to people without anyone else knowing the message exist. For example, e-

mailing can be used to send stegogrammes from one party to another party (recipient). Stegogrammes can also be share on internet forums between intended parties and the recipients can download the stegogramme from the forum and read it. It is also possible to send stegogrammes through social networking websites like facebook[3].

VIJAY and VISHAL proposed steganographic algorithm for bit (grayscale) or 24 bits (color image) based on logical operation. Their algorithm conceals MSB of a secret message (image) into LSB of the cover image. That n LSB of the cover image (original image), from a byte is changed by n MSB of secret message (image). The image quality of the stego-image, possible to improved low extra computational complexity. The worst case means square error between the stego-image (the result image) and the cover-image (original image) is derived [4]. Mohamed "et al." proposed quantizing the DCT coefficient using a predefined mathematical operation and then concealing the secret bits in all frequency pixels of the quantized DCT coefficient using least significant-bit (LSB) to allow a large message capacity [5]. Ramandeep and Ramanjot proposed an efficient authentication method for JPEG images based on Genetic Algorithms (GA). His authentication methods for JPEG images require the receivers, to know the quantization table beforehand in order to authenticate the images. The quantization tables used in the JPEG compression are different for various quality factors, subsequently increasing the burden on the receivers to preserve many of quantization tables [6]. Mohit and Neelu proposed a novel DCT-based steganographic method for hiding the data. Each bit of data is concealed by changing the least significant bit of low frequency DCT coefficients of cover image blocks [7].

## II. STEGANOGRAPHY REVIEW

Steganography explained as the art and science of hidden communication. Steganography insures possibility of sending secret messages, through use of available communications media, even under conditions that are monitored. There is the possibility of sending messages so that no one can detect the existence of secret messages. The concealing is done by weakening some characteristics of other media (image, text, audio), which is called the cover. Final output has equal properties to cover media, the cover contains the secret message, when secret message inside a cover image it will result is a stego-image, and when the secret message inside a video will the result is a stego-video and and so on. Two algorithms are needed to design steganography system, one for hiding data and other to extracting the data. The main goal in embedding algorithm is to conceal the secret message within the cover media without attracting

any notice. The extraction algorithm can be achieved by inverting the steps of embedding algorithm. The secret message (text file, image file, audio file or video file) which contains the secret information is first sent to the encoder unit. And the concealing of the secret message is done with few distortions and changes in the cover image. Usually a key is needed to increase the security level of the encoder unit and this same key is used in the extraction phase. Without using this key, the message will be extracted without any impediments, if someone guesses the embedding or extraction algorithm right. Then uses the each of the keys and the image in the embedding (encoding) process, are transmitted via a communication channel. Secret message is the final output of the extraction process, the steganogram can suffer changes the values of some bits due exposure to different types of noises during transmission via the communication channel.

There are two possible application steganographic tools: the spatial domain and the frequency domain. In the spatial domain, the concealment process is mostly carried out by bitwise manipulation. While, The frequency domain tools include those groups such as Discrete Cosine Transformation (DCT) and discrete wavelet transformation, that manage algorithms and image transforms.

In this paper, we combined two steganography algorithms namely JSteg algorithm and OutGuess algorithm, to enhance the protection level of hidden images. The secret message (image) is concealed inside an image by using Jsteg algorithm, then the resultant Jsteg-image is again hidden inside another image using OutGuess 0.1 algorithm. The tricky nature of hiding an already hidden image is using two different algorithms introduces some complexity and makes it more deceptive to a third party, hence reducing the suspension of in the existence of a secret image and significantly enhancing the protection level.

### III. SPATIAL DOMAIN STEGANOGRAPHY

Spatial domain techniques embed messages in the intensity of the pixels directly [8] [9] [10]. Least Significant Bit (LSB) is the first most widely used spatial domain steganography technique. It embeds the bits of a message in the LSB of the image pixels [11] [12]. But the problem with this technique is that if the image is compressed then the embedded data may be lost. Thus, there is a fear of loss of data that might have sensitive information [13] [7].

#### IV. TRANSFORM DOMAIN TECHNIQUES

##### 4.1 JPEG COMPRESSION:

For the implementation of image compression in the coordination of JPEG, first convert the RGB color coordination into the coordination of YUV. In this coordination the Y component refers to matching the brightness of a pixel and the U and V components refer to the color of a pixel [15]. Currie, D.L. & Irvine, C.E. Illustrate that the human eye is very sensitive to changes in brightness of pixels more than the changes in color of pixels [14]. Some samples are taken from the bottom of color data to reduce the file size when applying JPEG compression. The use of a factor 2 will reduce the size of the file, where the color components (U and V) are reduce by half in the horizontal and vertical directions [15].

Secondly, Discrete Cosine Transform (DCT) is used for the transformation of the image into JPEG, The DCT is a mathematical transform that converts a signal from coordination into frequency coordination, Through grouping the pixels into  $8 \times 8$  pixel blocks and converting the pixel blocks into 64 DCT coefficients each. That's where all 64 pixel images in that block will be affected when any DCT coefficient is modified.

Thirdly stage is the quantization of the compression. One form biological characteristics of the human eye can be exploited: that the human eye is rather good to distinguish between differences in brightness or (luminance) in low frequencies, but they are not good at distinguishing between differences in lighting or brightness in the high frequencies. This indicates that the strength of high frequency shrunk, without any effect on the appearance of the image. To further reduce the file size, the result is rounded to the integer values and the coefficients are encoded by using Huffman coding [15].

##### 4.2 JSteg

There are several features using images in JPEG format, an image used in Steganographic applications. First, the JPEG image file format has a large scale patronage and has become standard for storing and transmitting images on the network. When using JPEG images in the process of concealing data, the attention of the attacker or anyone else on the resulting image is less than that with most other formats. Second, considerable controls are available on the quantized image. Finally, JPEG file provides the ability to hide a large amount of steganographic

data messages. [16]. Derek Upham's JSteg was the first publicly available steganographic system for JPEG images [1].

Before starting the process of embedding, in JPEG image all  $8 \times 8$  blocks are converted to the frequency domain using DCT and then uses DCT to transform each block into DCT coefficients. In a request for the values that will be displayed whole numbers, each  $8 \times 8$  block is quantized according to a Quantization Table. Two types of coefficient could be seen on every  $8 \times 8$  block: DC and AC. It is known that value at the top left of each  $8 \times 8$  block refer to DC coefficient. It contains the mean value of all the other coefficients in the block, referred to as the AC coefficients. DC coefficients give a good estimate of the level of detail in the block because it is very important for each block. Therefore, no manipulation or changing of the DC coefficients values should happen, because it will lead to many changes of the values of the AC coefficients causing visual discrepancy when the image is converted back to the spatial domain and viewed normally. For this reason, the JSteg algorithm does not embed message data over any of the DC coefficients for every block. And also, the algorithm doesn't permit embedding on any AC coefficient equal to 0 or 1 [2] .

#### V. OUTGUESS 0.1

OutGuess 0.1 preserves statistics based on frequency counts and on this basis, it is not possible to detect steganographic contents. Before starting the process of concealing data, OutGuess can determine the maximum size of the message that we want to hide in another message, while still being able to maintain statistics based on frequency counts. Because the chi-square attack is based on analyzing first-order statistics of the stego image, therefore it cannot detect the concealed messages when an OutGuess algorithm is used [18]. Algorithm OutGuess 0.1 represents a process of concealment through a mixture of both the randomized Hide & Seek algorithm and the JSteg algorithm. Firstly, step is to convert the image to the DCT domain. Then, the coefficients are shuffled into a seemingly random order using a PRNG according to a seed. Then, message data is embedded by using the same technique as JSteg (JPEG image all  $8 \times 8$  blocks are converted to frequency domain using DCT and then uses DCT to transform each block into DCT coefficients. In a request for the displayed values to be whole numbers, each  $8 \times 8$  block is quantized according to a Quantization Table. Two types of coefficient could be seen on every  $8 \times 8$  block: DC and AC. It is known that value at the top left of each  $8 \times 8$  block refer to DC

coefficient.) before finally reversing the shuffle such that the coefficients are back in the correct positions. The image is then converted back into the spatial domain and thus the stegogrammes is produced. The algorithm still avoids embedding within the DC coefficient and any AC coefficient equal to either 1 or 0 [2]. The first version of OutGuess was designed by Neils Provos [17].

## VI. PROPOSED METHOD

In this paper, we combined two steganography algorithms namely JSteg algorithm and OutGuess algorithm, to make use of it to enhance the level of protection for the hidden images. The secret message (image) is concealed inside an image by using Jsteg algorithm and the resultant Jsteg-image is again hidden inside another image using OutGuess 0.1 algorithm. In other words, the secret message (image) twice hidden in two separate images, first using Jsteg algorithm, and secondly using Outguess 0.1 algorithm to hide the resulting jsteg image of the first operation, And the final product is the outguess-image. The tricky nature of hiding an already hidden image using two different algorithms introduces some complexity and makes it more deceptive to a third party, hence reducing the suspension of in the existence of a secret image and significantly enhancing the protection level. Figure(1) diagram explains the proposed method.

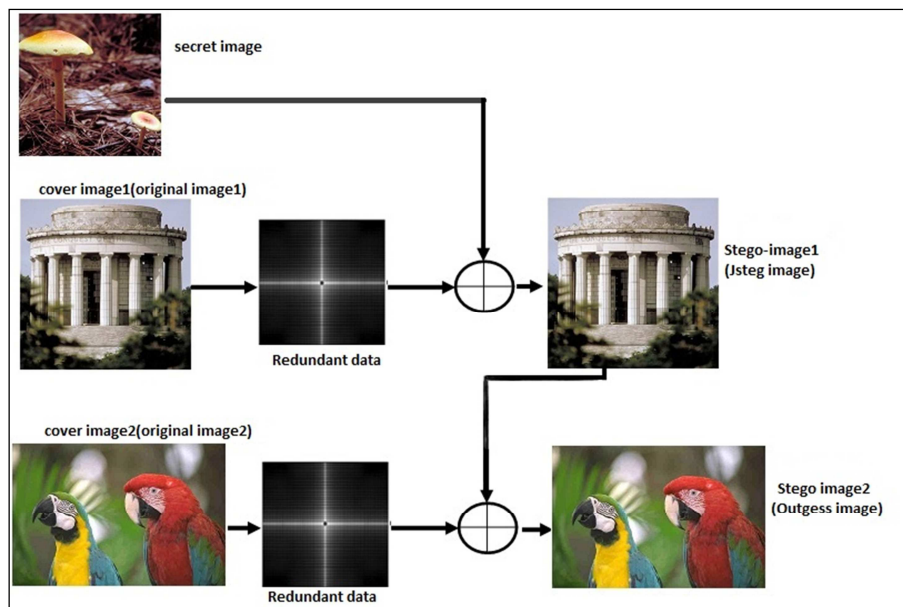


Fig1: Diagram explains the proposed method.

### 6.1 Embedding algorithm

Input: cover image1, cover image2, secret image1, secret image2

Step1: read cover image1. JPEG

- A. JPEG partitions a cover image1 into non overlapping blocks of 8\*8 pixels
- B. Calculate DCT coefficient for each block
- C. Quantize the coefficients

Step2: hiding process by using JSteg algorithm

While left to embed do

- A. Get next DCT coefficients from cover image1
- B. If  $DCT \neq 0$ ,  $DCT \neq 1$  &  $DCT \neq -1$  then
- C. Get LSB from the message
- D. Replace DCT LSB with message bit

End (if)

End (while)

Step3: calculate message capacity

Step 4: Writ JPEG image by de-quantize and take inverse DCT to obtain stego image1

Secret image2= stego image1

Step5: Read cover image2.JPEG

- A. JPEG partitions a cover image2 into non overlapping blocks of 8\*8 pixels
- B. Calculate DCT coefficient for each block
- C. Quantize the coefficients

Step6:hiding process by using Outguess algorithm

While left to embed do

- A. Get pseudo random DCT coefficient from cover image2
- B. If  $DCT \neq 0$ ,  $DCT \neq 1$  &  $DCT \neq -1$  then
- C. Get LSB from the message
- D. Replace DCT LSB with message bit

End (if)

End (while)

Step7: calculate message capacity

Step8: Write JPEG image by de-quantize and take inverse DCT to obtain stego image2.

The algorithm was implementation on Matlab 7.6 platform the results are shown in Figure (2) .And from the result we can see that the proposed approach successfully combined two steganographic methods in frequency domain, where an intended secret image (hidden image1) is first hidden using JSteg algorithm and the resultant image is again hidden in another image using OutGuess algorithm.



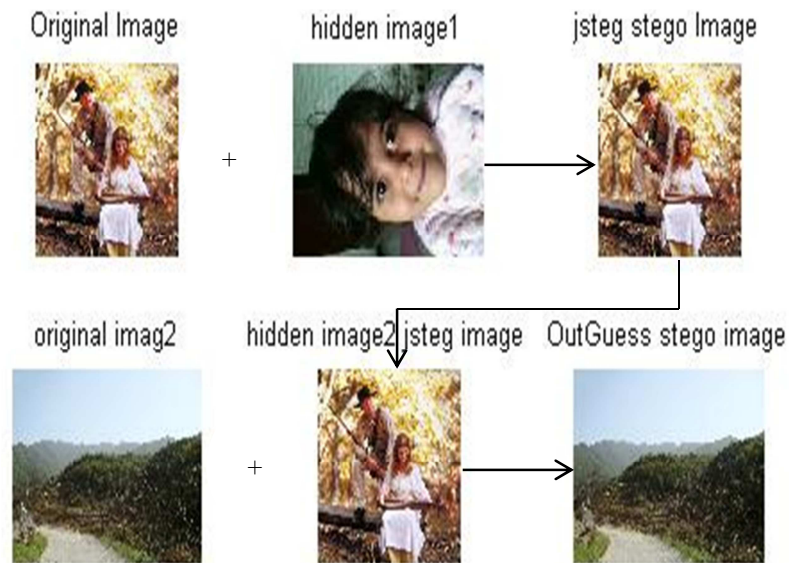


Fig2: Explain encoding process

## 6.2 Extracting algorithm

Input: Stego image2

Step1: read Stego image2.JPEG

- A. JPEG partitions Stego image2 into non overlapping blocks of 8\*8 pixels
- B. Calculate DCT coefficient for each block
- C. Quantize the coefficients
- D. Calculate message capacity

Step3: Extracting process by using Outguess algorithm

While left to embed do

- A. Get pseudo random DCT coefficient from Stego image2
- B. If  $DCT \neq 0$ ,  $DCT \neq 1$  &  $DCT \neq -1$  then
- C. Get LSB from the message
- D. Replace DCT LSB with message bit

End (if)

End (while)

Step4: Writ JPEG image by de-quantize and take inverse DCT to obtain secret image2.

Stego image1= Secret image2

Step5: Read Stego image1.JPEG

- A. JPEG partitions Stego image1 into non overlapping blocks of 8\*8 pixels
- B. Calculate DCT coefficient for each block
- C. Quantize the coefficients
- D. Calculate message capacity

Step6: Extracting process by using JSteg algorithm

While left to embed do

- A. Get next DCT coefficients from Stego image1
- B. If  $DCT \neq 0$ ,  $DCT \neq 1$  &  $DCT \neq -1$  then

## C. Concatenate DCT LSB to secret message

End (if)

End (while)

Step7: Write JPEG image by de-quantize and take inverse DCT to obtain secret image1.

After the implementation of this algorithm in Matlab 7.6 program the results obtained are shown in Figure (3):

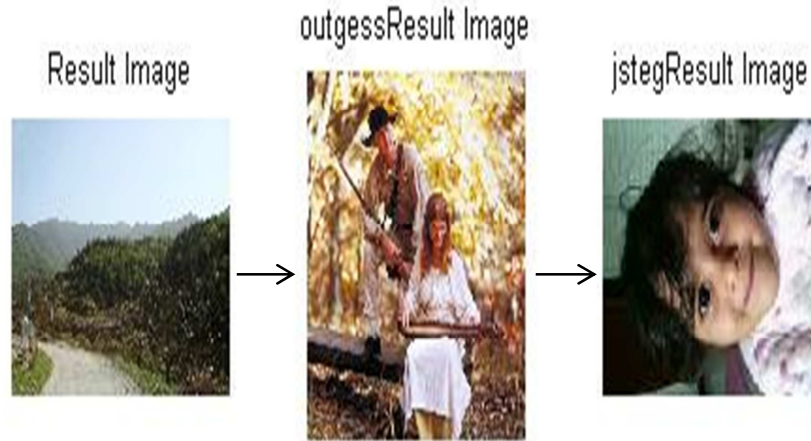


Fig3: Explain decoding process

## VII. EXPERIMENTAL AND RESULTS

The experiments were implemented on a set of images downloaded from the images database at Washington university [23, 28, 29] and Oklahoma University [24, 30] (more than 500 images of JPEG type) and also some images from the special camera. Fundamental information hiding systems: capacity, security, and durability. The capacity is the amount of data that is possible to be hidden in a cover medium. Security refers to the inability of the attacker to detect hidden data. Robustness refers to the extent to which the stego medium can withstand the attacker, which can destroy the hidden information.

**Embedding Capacity**

It is the maximum size of the secret data that can be embedded in the cover image without deteriorating the integrity of the cover image. It can be represented in bytes or Bit Per Pixel(bpp), The calculated explain in equation 1.

$$\text{capacity} = (X * Y) / 64 * b * (n - 15) \quad (1)$$

In this equation, X and Y are the dimensions of the cover image. By dividing the product of X, Y by 64, the number of 8\*8 blocks is achieved. During data embedding process, no data are

embedded in the last 15 coefficients, so the term (n-15) is used here, and in each coefficient b bits of data will be embedded.

### Peak-signal-to-noise ratio (PSNR)

As a performance measurement for image distortion, the well known peak-signal-to-noise ratio (PSNR) which is classified under the difference distortion metrics is applied to the stego-images. It is defined as Eq (2):

$$PSNR = 10 \log_{10} \left( \frac{C_{max}^2}{MSE} \right) \quad (2)$$

Where MSE denotes mean square error which is given as Eq (3):

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2 \quad (3)$$

Table (1) illustrates the capacity and PSNR for the encoding process (1).

Table1.Capacity and PSNR for images

	Image	Capacity	PSNR
Encoding process1	Outguess stego-image Stego	1043768	56.8607

Where x and y are the image coordinates, M and N are the dimensions of the image,  $S_{xy}$  is the generated stego-image and  $C_{xy}$  is the cover image. Also  $C_{max}^2$  holds the maximum value in the image, for example:

$$C_{max}^2 \leq \begin{cases} 1, & \text{double precision} \\ 255, & \text{unit 8 bit} \end{cases}$$

Many authors [19 - 27], consider  $C_{max}=255$  as a default value for 8 bit images. It can be the case, for instance, that the examined image has only up to 253 or fewer presentations of gray colors. Knowing that  $C_{max}^2$  results in a severe change to the PSNR value. This  $C_{max}$  can be defined as the actual maximum value rather than the largest possible value. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 40 dB and above. In this paper, after combining two concealment algorithms specifically JSteg and OutGuess algorithm. We use the OutGuess 0.1 algorithm to further enhance the level of protection for detection of a secret message (image), which has already been hidden inside another image using an Jsteg algorithm. And as such, the tricky nature

of hiding an already hidden image is using two different algorithms introduces some complexity and makes it more deceptive to a third parties. This in effect reduces the suspension in the existence of the secret image, thereby significantly enhancing the image protection level.

The hidden image (size image  $<130 \times 130$ ) will be stored two times. The first time by using jsteg algorithm and the second time hiding the resultant image (Jsteg stego) using outguess algorithm. The capacity is calculated two times to get the hidden image. The first time for Jsteg and the second time for OutGuess and this is another factor adding safety to the secret image. The results of the PSNR values of the Stego-images calculated after sending the final Stego-images via e-mail to another computer, and retrieving the hidden messages (image), were between (50-57)db and this range is considered to be a very good and acceptable steganography system. Fig(5) is an illustration of the encoding processes, and as shown in table(2) explaining the PSNR & capacity for some encoding processes. Fig(5) explain coefficient histogram for cover image and final stego image.

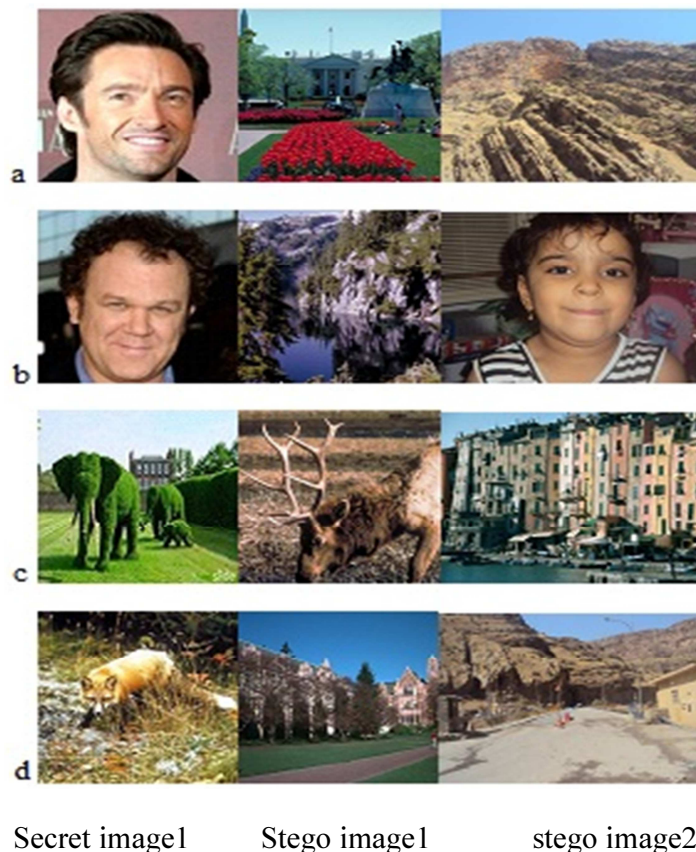
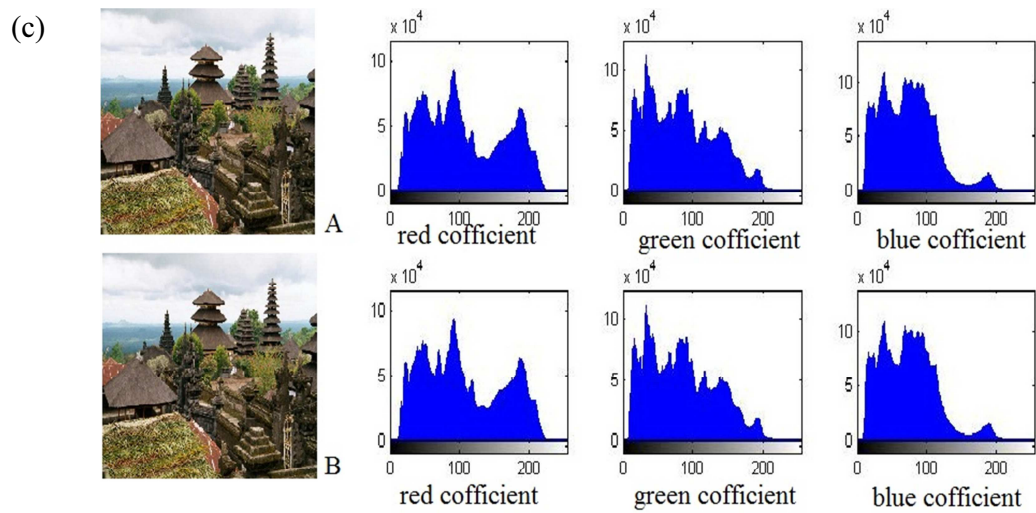


Fig4: illustrate for some of encoding processes (a) encoding process1, (b) encoding process2,



Fig(6): Coefficient histogram for (A) cover image (B) outguess steganogram

encoding

3and (d) encoding process 4.

process

Table2. Explain PSNR & capacity for some encoding processes.

Encoding process	Image	Capacity	PSNR
A	Outguess stego-image	1034728	57.8352
B	Outguess stego-image	1325120	59.6505

C	Outguess stego- image	1037432	55.8158
D	Outguess stego- image	2546416	54.3120

Table (3) show that PSNR of our proposed technique is better than proposed technique in reference [25-27], because the PSNR value of our technique exceed that of the previous technique with a significant margin. Depending on the result of the comparison, we find that the proposed method is good and acceptable and safe steganography scheme.

Table(3):comparison between our proposed method with the results of technique in refrencep[25].

Cover image	Previous results	<b>proposed method</b>
	PSNR (dB)	PSNR (dB)
Lena	<b>41.79</b>	<b>53.1257</b>
Baboon	<b>37.90</b>	<b>50.0200</b>
Airplane	<b>40.60</b>	<b>53.0196</b>
Peppers	<b>40.97</b>	<b>53.1825</b>

## VIII. CONCLUSIONS

This paper presented a steganographic approach that combined jsteg and outguess algorithms. The approach allowed us to benefit from the potential features and strengths of both algorithms and this added a significant level of protection to hidden images. In principle what happened in our proposed approach is that an image intended to be a secret image is first hidden in an image using jsteg algorithm and the resultant stego image is further hidden in another

second image using outguess 0.1 algorithm to produce a final stego image. The act of hiding an already hidden image (stego image) in another image alone is tricky and deceptive for a third party. Besides that, the idea of combining two steganographic algorithm makes the approach more complex for a third party and this increases the chances that the intended secret message (secret image) could go unnoticed.

Furthermore, the priority given to selecting a good image sizes and type further disguises the secret image and makes it more difficult for a third party to suspect the existence of a secret image. The experimental results indicated an average PSNR value of more than 50 dB for more than 100 images and that is a good and acceptable steganography scheme. As future work, we could try the combination of other steganography techniques and compare the efficiency levels, as well as adding image encryption.

## REFERENCES

- [1] Niels Provos and Peter Honeyman "Hide and Seek: An Introduction to Steganography" , *IEEE Computer Society* ,Vol.1,No.3, 2003,pp.32-44.
- [2] Philip Bateman and Dr. Hans "Image Steganography and Steganalysis", M.S., Department of Computing Faculty of Engineering and Physical Sciences, University of Surrey Guildford Surrey, United Kingdom, 2008.
- [3] Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani "Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm ",*International Journal of Computer and Electrical Engineering*, Vol. 4, No. 4, August 2012
- [4] Vijay and Vishal" A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection", *Theoretical and Applied Information Technology*, Vol. 36, No.1,2012
- [5] Mohamed Amin, Hatem M. Abdulkader, Hani M. Ibrahim, and Ahmed S. Sakr1"A Steganographic Method Based on DCT and New Quantization Technique", *International Journal of Network Security*, Vol.16, No.3, PP.214-219, May 2014
- [6] Ramandeep Kaur Toor and Ramanjot Kaur"A Steganographic Method Based Upon JPEG and Quantization Table Modification", *International Journal of Information Technology and*

*Knowledge Management* ,NO.1,Vol.6, pp. 19-21, 2012

[7] Mohit Kumar Goel & Neelu Jain “ A Novel Steganographic Technique Based on LSB-DCT Approach” , in *National Conference on Emerging Trends in Information and Computing Technologies* NCETICT, 2012.

[8] Chan, C.K. and Cheng. L.M. “Hiding Data in Image by Simple LSB Substitution”, *Pattern Recognition*, No.3, Vol.37, pp. 469 – 474, 2004.

[9] Chang,C.C and Tseng, H.W. “A Steganographic Method for Digital Images Using Side Match”, *Pattern Recognition Letters*,No.12, Vol.25, pp. 1431 – 1437, 2004.

[10] Sayuthi Jaafar, Azizah A Manaf, Akram M Zeki, “Steganography Technique Using Modulus Arithmetic”, in *9th International Symposium on Signal Processing and Its Applications*, pp. 1 – 4, 2007.

[11] W. Bender, D. Gruhl, N. Morimoto, and A. Lu,” Techniques for Data Hiding”, *I.B.M. Systems Journal*, No.3.4,Vol.35, pp. 313-336, 1996.

[12] N. Nikolaidis, and I. Pitas, “Robust Image Watermarking in the Spatial Domain”, *Signal Processing*, No.3,Vol.66, pp. 385-403, 1998

[13] T. Morkel, J. Eloff, and M. Olivier,”An Overview of Image Steganography”, *In Proceedings of the Fifth Annual Information Security South Africa Conference ISSA*, 2005.

[14] Currie, D.L. & Irvine, C.E., “Surmounting the Effects of Lossy Compression on Steganography”, in *19th National Information Systems Security Conference*, 1996

[15] D. Fu, Y. Shi, D. Zou, and G. Xuan. "JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain", *IEEE: 8th Workshop on Multimedia Signal Processing* 2006, pp. 310-313, 2006.

[16] Tao Zhang & Xijian Ping “A Fast and Effective Steganalytic Technique against JSteg-like Algorithms” *SAC* 2003.

[17] N. Provos. "Defending Against Statistical Steganalysis", *10th USENIX Security Symposium*, vol. 10, pp. 323-335, 2001

[18] Fridrich J., Goljan M., and Hoge D., “Attacking the OutGuess,” ,*Proc.ACM Workshop Multimedia and Security*, 2002.

[19] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt ”Digital image steganography: Survey and analysis of current methods” , *Signal Processing*, No.3,Vol.90, pp 727–752,2010.

[20] X. Li, J. Wang, “A Steganographic Method Based Upon JPEG and Particle Swarm



Optimization Algorithm”, *Information Sciences*, No.15, Vol.177, pp. 3099–31091, 2007.

[21] S.C.Mukhopadhyay, F.P.Dawson, M.Iwahara and S.Yamada, “A Novel Compact Magnetic Current Limiter for Three Phase Applications”, *IEEE Transactions on Magnetics*, Vol. 36, No. 5, pp. 3568-3570, September 2000.

[22] Y.H. Yu, C.C. Chang, I.C. Lin,” A New Steganographic Method for Color and Grayscale Image Hiding”, *Computer Vision and Image Under- standing*, No.3, Vol.107, pp.183–194,2007.

[23] S.C.Mukhopadhyay, S. Deb Choudhury, T. Allsop, V. Kasturi and G. E. Norris, “Assessment of pelt quality in leather making using a novel non-invasive sensing approach”, *Journal of Biochemical and Biophysical methods*, Elsevier, JBBM Vol. 70, pp. 809-815, 2008.

[24] A.I. Hashad, A.S. Madani, A.E.M.A.” Wahdan, A Robust Steganography Technique Using Discrete Cosine Transform Insertion”, in *IEEE/ITI Third International Conference on Information and Communications Technology*, 2005, pp. 255–264.

[25] [http://www.cs.washington.edu/research/imagetdatabasgroundtruth\\_tars.for.download](http://www.cs.washington.edu/research/imagetdatabasgroundtruth_tars.for.download)

[26] <http://vision.okstate.edu/loc=csiq>

[27] N.K. Suryadevara, S.C. Mukhopadhyay, R. Wang, R.K. Rayudu, Forecasting the behavior of an elderly using wireless sensors data in a smart home, *Engineering Applications of Artificial Intelligence*, Volume 26, Issue 10, November 2013, Pages 2641-2652, ISSN 0952-1976, <http://dx.doi.org/10.1016/j.engappai.2013.08.004>.

[28] V.Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz” Color Image Steganography based on Pixel Value Modification Method Using Modulus Function” *International Conference on Electronic Engineering and Computer Science*, IERI Procedia 4, 2013, pp. 17 – 24.

[29] Yanmin LUO, Peizhong LIU and Minghong LIAO, An artificial immune network clustering algorithm for mangroves remote sensing, *International Journal on Smart Sensing and Intelligent Systems*, VOL. 7, NO. 1, pp. 116 – 134, 2014.

[30] Daode Zhang et al., Research on chips’ defect extraction based on image-matching, *International Journal on Smart Sensing and Intelligent Systems*, VOL. 7, NO. 1, pp. 321 – 336, 2014.